2023 BSA State Legislative Summary: CYBERSECURITY

- 43 states considered 245 cybersecurity bills in 2023. That is fewer than the 293 in 2022.
- 43% more cybersecurity bills were enacted in 2023 (43) than in 2022 (30). However, only about 18% of cybersecurity bills were enacted overall.
- Cybersecurity bills were enacted on various topics in cybersecurity, but the most common were breach notification, incident reporting, incident response, intergovernmental cooperation, and third-party applications.
- Several states also passed laws for cybersecurity funding, addressing workforce challenges, updating protocols, tackling ransomware, and establishing affirmative defense laws.
- Arkansas established the Self-Funded Cyber Response Program for participating state and local governments to provide coverage for cybersecurity incidents and risks.
- Although 32 cybersecurity infrastructure bills were introduced, only one was enacted. Conversely, however, 13 incident reporting and response bills were introduced and seven were enacted.
- 14 bills related to intergovernmental cooperation on cybersecurity issues were introduced and three were enacted.

States continued to address various cybersecurity concerns, focusing primarily on public sector concerns. Top public sector concerns in state legislatures were breach notification bills, improving intergovernmental cooperation, updating protocols, and tackling ransomware. States also looked to address cybersecurity issues in the private sector including addressing workforce challenges, establishing criminal penalties, modifying breach notifications, and banning or setting requirements for third-party applications and devices. However, states introduced 16% fewer cybersecurity bills in 2023 than in 2022, despite an increase in the number of states introducing cybersecurity bills and on a wider variety of topics. Additionally, cybersecurity bills were overwhelmingly likely to be introduced by a member of the majority party, regardless of partisan control.

Forty-three states, 86%, have introduced legislation related to cybersecurity in 2023. The only states that did not are Alabama, Alaska, Colorado, Delaware, Maine, Michigan, and New Hampshire. Most state cybersecurity bills related to creating or improving the state's cybersecurity infrastructure or updating data breach notification laws. Together, these represent about a quarter of all introduced cybersecurity bills. Although more states continue to introduce cybersecurity legislation across a wider variety of topics, the overall quantity of cybersecurity bills dropped 16% from 2022 to 2023. As in 2022, Massachusetts and New York both introduced a large quantity of bills; however, Texas and Iowa are now the top-introducing states for cybersecurity bills. The four states (Iowa, Massachusetts, New York, and Texas), account for almost 40% of all cybersecurity bills introduced. Notably, Texas did not have a legislative session in 2022 and will not in 2024. Enacted legislation demonstrates the bipartisan nature of cybersecurity across the states. Of the enacted bills, Republicans introduced 18, Democrats introduced 14, and committees or departments introduced eight. Almost exclusively, majority party introduced the enacted legislation, regardless of party.

More specifically, states introduced significantly more data breach legislation—29 bills in 13 states. As was typical, data breach bills were introduced by the majority party and were bipartisan in nature. Five bills in five states (Montana, Pennsylvania, Rhode Island, Texas, and Utah) that were enacted modified breach notification laws and three of them were related to private sector. In the private sector, Utah added organizations to the breach notification process, whereas Texas modified the notification process to the state's attorney general. Pennsylvania adopted insurance data breach notification laws. Montana agencies must report breaches to the governor. Rhode Island reduced the time for government to report data breaches from 45 to 30 days.

Incident reporting and response bills were only 5% of bills, but more than 50% of introduced bills were enacted. Three of those bills were about incident response, three were about reporting, and one was about both. Kansas enacted a bill to add requirements for significant cyber incidents. It additionally provides for cybersecurity requirements, training, assessments, and incident response. Other response bills ranged from Indiana establishing the Indiana Cyber Civilian Corps Program to New Jersey requiring a plan to address internet outages caused by cyberattacks. Arkansas enacted a bill to regulate policies and reports to address cybersecurity incidents. New Jersey and Texas modified their cybersecurity incident reporting laws for state agencies, whereas Maryland modified it for public utilities.

Cybersecurity infrastructure bills comprised 13% of cybersecurity bills, but only one was enacted in Arkansas. These bills typically deal with creating the framework in the state, local government, or state agencies to safeguard against cyberattacks and provide appropriate protocols. These bills were often paired (Hawaii, New York, Texas) with assessing the state's current cybersecurity.

Seventeen cybersecurity funding measures were introduced, but only three were enacted, including $10 million for the Arkansas Self-Funded Cyber Response Program, which was approved in a separate bill. The program is designed to provide coverage for cybersecurity incidents and risks, damages, or losses caused by a cyberattack against participating governments. Massachusetts appropriated funds to the Executive Office of Technology Services and Security. Finally, Oregon established the Oregon Cybersecurity Center of Excellence and state Cybersecurity Workforce Development Cybersecurity Grant Program Funds.

Several states looked to modify laws related to cybersecurity procurement, most often related to local governments being able to procure cybersecurity products. Massachusetts introduced a bill giving preference to vendors that carry cybersecurity insurance.

Fifteen bills related to education and training about cybersecurity awareness were introduced and four were enacted in Arkansas, Kansas, North Dakota, and Washington. The Arkansas, Kansas, and Washington bills focused on training for public sector employees, whereas North Dakota's bill focused on cybersecurity education in high school. A similar education bill in California has passed both chambers. The introduced bills typically focused on training public sector education, but a few did focus on general awareness and education.

In 2024, the state activity on cybersecurity will continue on various issues, with a focus on public sector activities, including breach notification, incident reporting and response, and procurement.

FOR MORE INFORMATION CONTACT:
Matthew Lenz | Senior Director, State Advocacy | matthewl@bsa.org
Abigail Wilson | Manager, State Advocacy | abigailw@bsa.org